

DeFi

"Express Mail" mailing label number R13889292679US

Date of Deposit December 16, 1993
I hereby certify under 37 CFR 1.10 that this correspondence is being deposited with the United States Postal Service as "Express Mail Post Office to Addressee" with sufficient postage on the date indicated above and is addressed to the Commissioner of Patents and Trademarks, Washington, D.C. 20231.

Elizabeth K. Donohoe
Elizabeth K. Donohoe

DIGITAL ACTIVE ADVERTISING

BACKGROUND OF THE INVENTION

5 The recent rapid growth of information applications
on international public packet-switched computer networks
such as the Internet suggests that public computer networks
have the potential to establish a new kind of open
marketplace for goods and services. Such a marketplace
10 could be created with a network sales system that comprises
a plurality of buyer and merchant computers, means for the
users of the buyer computers to display digital
advertisements from the merchant computers, and means for
the users to purchase products described by the
15 advertisements.

A network based sales system will need to allow
users to preview products at little or no cost, and will
need to make a large number of product advertisements
available in a convenient manner. In addition, the shopping
20 system will need to include easy-to-use facilities for a
user to purchase desired products using a merchant
independent payment method. In addition the network sales
will need to allow new buyers and merchants to enter the
market.

25 A central requirement for a marketplace is a payment
mechanism, but at present no merchant independent payment

mechanism is available for computer networks that permits users to utilize conventional financial instruments such as credit cards, debit cards, and demand deposit account balances. We expect that both retail payment and wholesale payment mechanisms will be required for networks, with consumers using the retail mechanism for modest size purchases, and institutions using the wholesale mechanism for performing settlement between trading partners. For wide acceptance the retail mechanism will need to be a logical evolution of existing credit-card, debit-card, and Automated Clearing House facilities, while for acceptance the wholesale mechanism will need to be an evolved version of corporate electronic funds transfer.

These problems of have been approached in the past by network based sales systems wherein, for example, each merchant maintains an account for each user. A user must establish an account with each merchant in advance in order to be able to utilize the merchant. The prior art network based sales systems are not designed to allow users to use their existing credit card and demand deposit accounts for payment, nor are they designed to allow for programs to be included in digital advertisements.

According, therefore, it is a primary objective of this invention to provide a user interactive network sales system in which the user can freely use any merchant of

choice and utilize existing financial instruments for
payment. Other objects include a network sales system which
provides a high-quality user interface, which provides users
with a wide variety and large volume of advertisements,
5 which is easily extensible to new services, and which is
easily expanded to new applications within the existing
infrastructure of the system.

Still other objects of the invention are to provide
a network payment system that will authorize payment orders
10 and remove part of the risk of fraud from merchants.

An unavoidable property of public computer networks
is that they are comprised of switching, transmission, and
host computer components controlled by many individuals and
organizations. Thus it is impossible for a network payment
15 system to depend upon a specified minimum required degree of
software, hardware, and physical security for all of the
components in a public network. For example, secret keys
stored in a given user's personal computer can be
compromised, switches can be tampered with to redirect
20 traffic, and transmission facilities can be intercepted and
manipulated.

The risk of performing retail payment in a public
network is compounded by statutes that make a payment system
operator in part liable for the security lapses of its
25 users. Existing Federal statutes in the United States,

including the Electronic Funds Transfer Act and the Consumer Credit Protection Act, require the operator of a payment mechanism to limit consumer liability in many cases.

Payment system operators may have other fiduciary
5 responsibilities for wholesale transactions. Similar responsibilities exist in other countries for retail and wholesale transactions.

In existing credit card payment systems, a credit card's issuing bank takes on the fraud risk associated with
10 misuse of the card when a merchant follows established card acceptance protocols. Acceptance protocols can include verifying a card holder's signature on the back of their card and obtaining authorization for payments over a certain value. However, in network based commerce a merchant can
15 not physically examine a purchasers credit card, and thus the fraud risk may revert to the merchant in so called "card not present" transactions. Many merchants can not qualify to take this risk because of their limited financial resources. Thus the invention is important to allow many
20 merchants to participate in network based commerce.

Other objects of the invention include utilizing existing financial instruments such as credit cards, debit cards, and demand deposit accounts for merchant payments.

Existing network payment systems do not connect to
25 the financial system for authorization and are not

compatible with conventional financial instruments.

Existing network payment systems include the Simple Network Payment Protocol [Dukach, S., SNPP: A Simple Network Payment Protocol, MIT Laboratory for Computer Science, Cambridge,

5 MA, 1993.], Sirbu's Internet Billing Server [Sirbu, M. A., Internet Billing Service Design and Prototype

Implementation, Information Networking Program, Carnegie-Mellon University, 1993], and NetCash [Medvinsky, G., and Newman, B. C., NetCash: A Design for Practical Electronic

10 Currency on the Internet, Proc. 1st ACM Conf. on Comp. and Comm. Security, November, 1993].

A further object of the invention is to allow users in an untrusted network environment to use conventional financial instruments without requiring modification to
15 existing financial system networks.

The following definitions apply to the present invention. A principal is a person, company, institution, or other entity that is authorized to transact business as part of a network payment system. A payment order describes
20 the identity of a sender, a payment amount, a beneficiary, and a sender unique nonce. A sender is a principal making a payment. A beneficiary is a principal to be paid by the payment system. A sender unique nonce is an identifier that is used only once by a given sender. An example of sender
25 unique nonces are unique timestamps. An external account is

an account that can be used to settle a payment order for either a sender or a beneficiary in the external financial system. Examples of external accounts include demand deposit accounts and credit card accounts. An external
5 device is a physical object that is kept in the possession of a user for the purpose of identifying the user.

A network payment system is a service that authorizes and executes digital payment orders that are backed by external accounts. A payment system authenticates
10 a payment order, checks for sufficient funds or credit, and then originates funds transfer transactions to carry out the payment order. A payment system acknowledges acceptance or rejection of a payment order. More than one payment system may exist on a given network, and a given payment
15 system may operate on more than one host to increase its reliability, availability, and performance. An authenticator is a digital value that is appended to a payment order and becomes part of the payment order that authenticates the payment order as genuine.

20 SUMMARY OF THE INVENTION

The invention relates to a network sales system for enabling users to purchase products using a plurality of buyer computers that communicate over a network with a plurality of merchant computers. Each merchant computer
25 has a database of digital advertisements. Each digital

advertisement includes a price and a product abstract.
Buyer computers request, display, and respond to digital
advertisements from merchant computers. Users can purchase
products with their buyer computers after they have
5 specified an account to pay for the purchase. A network
payment service is used to authorize the purchase before
merchant fulfillment is performed.

In a particular aspect of the invention, the merchant
computer can request account information when it is not
10 provided by the buyer computer. In another aspect of the
invention, the buyer computer can present to a merchant a
pre-authorized payment order that is obtained from a network
payment system.

In another aspect of the invention, an electronic
15 sales system contains digital advertisements that include
programs. The programs are executed on behalf of a user by
a buyer computer, and can lead to a purchase request
directed to a merchant computer that performs product
fulfillment.

20 In another aspect of the invention a network payment
system executes payment orders. A payment order includes a
sender, a beneficiary, a payment amount, and a nonce
identifier. A payment order is signed by a client computer
with an authenticator that is checked by the payment system.
25 Payment orders are backed by accounts in the banking

system, and are authorized by the network payment system by sending messages into a financial authorization network that knows the status of these accounts. The payment system accomplishes settlement by sending messages into an existing
5 financial system network.

In another aspect, payment orders are authenticated based on the delivery address they specify. In another aspect, the payment system will specify in its authorization legal delivery addresses. In another aspect, authenticators
10 for payment orders are based on one-time transaction identifiers that are known only to the user and the payment system. In another aspect, payment orders for a given sender are only accepted from certain client computer network addresses. In another aspect, the network payment
15 system sends messages into a financial authorization system in real-time before the network payment system will authorize a payment order.

BRIEF DESCRIPTION OF THE DRAWINGS

Other objects, features, and advantages of the
20 invention will appear from the following description taken together with the drawings in which:

Figure 1 is a block diagram of a typical network sales system in accordance with the invention;

Figure 2 is a screen snapshot of a buyer computer
25 display of an overview page from a merchant computer;

Figure 3 is a screen snapshot of a buyer computer display of a page of digital advertisements from a merchant computer;

Figure 4 is a screen snapshot of a buyer computer display of an account query page;

Figure 5 is a screen snapshot of a buyer computer display of a fulfillment page;

Figure 6 is a flow chart illustrating the processing of a sale between a buyer computer and a merchant computer;

Figure 7 is a flow chart illustrating the alternate processing of payment order means for obtaining missing payment information;

Figure 8 is a screen snapshot of a buyer computer display of an overview page from a merchant computer that contains a query input by the user;

Figure 9 is a screen snapshot of a buyer computer display of digital advertisements in response to a user's query;

Figure 10 is a screen snapshot of a buyer computer screen of a purchase confirmation;

Figure 11 is a screen snapshot of a buyer display of a fulfillment page like Figure 5;

Figure 12 is a flow chart illustrating an alternate processing of a sale between a buyer computer and a merchant computer where a payment order is pre-authorized;

Figure 13 is a block diagram of a typical network payment system in accordance with the invention;

Figure 14 is a flow chart illustrating the authentication, authorization, and settlement of a payment order;

Figure 15 is a flow chart illustrating an alternate processing of the authentication and verification of a payment order where transaction identifiers are used; and

Figure 16 is a flow chart illustrating an alternate processing of the authorization of a payment order where real-time approval from the financial authorization network may not be obtained.

DESCRIPTION OF A PARTICULAR PREFERRED EMBODIMENT

A network sales system 200 as shown in Figure 1 employs a network 67 to interconnect a plurality of buyer computers 61 and 62, merchant computers 63 and 64, each merchant computer with respective digital advertisement databases 65 and 66, and a payment computer 68. A user of the system employs a buyer computer to retrieve advertisements from the merchant computers, and to purchase goods of interest. A payment computer is used to authorize a purchase transaction.

A digital advertisement includes a product description and a price. In digital advertisement database

65 prices and descriptions may be stored separately, and one price may apply to many product descriptions.

In an alternate embodiment, the network sales system further includes external devices that are kept in the possession of users so that the users can authenticate themselves when they use a buyer computer.

The software architecture underlying the particular preferred embodiment is based upon the hypertext conventions of the World Wide Web. Appendix A describes the Hypertext Markup Language (HTML) document format used to represent digital advertisements, Appendix B describes the HTML forms fill out support in Mosaic 2.0, Appendix C is a description of the Hypertext Transfer Protocol (HTTP) between buyer and merchant computers, and Appendix D describes how documents are named with Uniform Resource Locators (URLs) in the network of computers. A document is defined to be any type of digital data broadly construed, such as multimedia documents that include text, audio, and video, and documents that contain programs.

Figure 2 shows an overview screen that has been retrieved from a merchant computer by a buyer computer and displayed by the buyer computer. It includes links 1, 2, and 3 that when activated by a user cause the buyer's computer to take specified actions. In the case of link 1, the document shown in Figure 3 is retrieved from a merchant

computer and displayed. In the case of link 2, a short audio segment is retrieved from a merchant computer and played. In the case of link 3, the query that can be entered into the query dialog box 4 is sent to a merchant
5 computer, and a document is retrieved from the merchant computer and displayed.

Figure 3 shows a document that contains three digital advertisements. The digital advertisements have been retrieved from the merchant computer after the
10 activation of link 3. The merchant computer may set the prices contained in the advertisements based on the on the identity of the user as determined, for example, by the network address of the requesting buyer computer. The document includes links 5, 6, and 7 that are used to
15 purchase the products described by the advertisements. For example, if link 5 is activated the missing payment information document shown in Figure 4 is retrieved from the merchant computer and displayed.

Figure 4 is a missing payment information document
20 that is used to gather user account information for the requested purchase in an HTML form. Radio buttons 8, 9, 10, 11, 12 are used to select a means of payment, dialog box 13 is used to enter an account number, dialog box 14 is used to enter an optional authenticator for the account, purchase
25 button 15 is used to send the account information to the

merchant computer and proceed with the purchase, link 16 is used to abort the purchase and return to the document shown in Figure 2, and dialog box 17 is used to enter optional user information that is associated with the purchase and ultimately used by a financial institution as part of a textual billing identifier for the purchase transaction. If provided, this additional information is included in the payment order for the purchase.

Figure 5 is a fulfillment document 18 that is produced once valid account information is provided to the missing payment information document in Figure 4 and purchase button 15 is activated.

Figure 6 is a flowchart that more fully describes the information flow in the purchase transaction shown in Figures 2 to 5. An initial user inquiry 19 from activating link 1 results in the HTTP request 20 for a specific document with a specified URL. The URL specifies the name of the merchant computer. The merchant computer retrieves the document given the URL at 21, and returns it to the buyer computer at 22. The buyer computer displays the resulting HTML document at 23. When the user activates link 5, an HTTP request 25 is sent to the merchant computer requesting the document.

In an alternate embodiment, document 22 is executed at 23 as a program. A program is defined as a set of

instructions that can exhibit conditional behavior based upon user actions or the environment of the buyer computer. As is known to those skilled in the art, there are many techniques for representing programs as data. The program
5 can be interpreted or it can be directly executed by the buyer computer. The program when executed will cause the buyer computer to interact with the user leading to the user purchase request 24, and the purchase message 25.

The merchant computer then attempts to construct a
10 payment order at 26 using the information it has gathered about the user. The buyer computer may have previously supplied certain credentials using fill out forms or other account identification means such as providing the network address of the buyer computer in the normal course of
15 communication. If the buyer computer is able to construct a complete payment order at 26 the payment order is sent to a payment computer for authorization at 27. If a payment order can be constructed, processing continues at 28.

Alternatively, the buyer computer may construct the
20 payment order at 24 and send it to the merchant computer at 25. In this case, the payment order assembly steps at 26, at the merchant computer, may only need to forward the payment order from the buyer computer.

A payment order includes user account information,
25 merchant account information, an amount, and a nonce

identifier that has not been previously used for the same user account. Variations of payment orders can be constructed, including payment orders that specify user or merchant identifiers in place of account information,
5 payment orders that specify a valid time period, payment orders that specify foreign currencies, and payment orders that include comment strings. Part of the process of constructing a payment order is creating a corresponding authenticator using one of the authenticator methods
10 described below.

In the illustrated embodiment of Figures 3 and 4, the merchant computer does not have sufficient information to construct a payment order at 26 and thus at 33 (Figure 7) constructs and returns a missing payment information
15 document in response to request 25. Operation 33 includes in the constructed document appropriate form fields based on what information the merchant computer has already collected from the user. The document is returned to the buyer computer at 34 and is displayed at 35. When the user
20 presses the purchase button 15, the contents of the form are transmitted to the merchant computer, at 36, to a specific URL name, using an HTTP request. Based on the supplied form fields, the merchant computer constructs a complete payment order. Alternatively, the buyer computer may construct the
25 payment order at 35 and send it to the merchant computer as

part of step 36. In this case, the payment order assembly steps 37 at the merchant computer simply passes on the payment order from the buyer computer. The payment order is sent to the payment computer in a message at 38.

5 In either case, the flowchart continues in Figure 6 where the payment computer checks the authorization of the payment order at 28. If the payment system authorizes the request, an authorization message at 29 is returned to the buyer computer, and the merchant computer checks at 30 that
10 the authorization message came from the payment computer using the authenticator mechanism described below. Assuming that the authorization message is valid, the merchant computer performs fulfillment at 30, returning the purchased product in response at 31. In our example in Figure 5 the
15 response at 31 is document 18 that was the logical target of link 5. If the payment system does not authorize the payment order then response 31 is a rejection of the user's purchase request.

In an alternate embodiment, step 30 can encrypt the
20 document using a key that is known to the buyer computer. As is known to those skilled in the art, the key can be communicated to the merchant computer using convention key distribution protocols. In this manner the document will be protected from disclosure to other users.

The fulfillment step at 30 can alternatively schedule a physical product to be shipped via ordinary mail or other means. This can be accomplished by updating a fulfillment request database or by sending a message to a shipping system. In this case the response at 31 is a confirmation that the product has been scheduled to ship. In this way the network sales system can implement an electronic mail order system.

Figures 8, 9, 10, and 11 show a second example that uses query based access to digital advertisements. It is assumed that the previous example was used by the user immediately before at the same buyer computer.

Figure 8 shows the overview screen where the query "movie review" has been entered into dialog box 39. When the user activates process button 40, the merchant searches databases as described by the URL attached to button 40, and creates a response document as shown in Figure 9.

Figure 9 shows digital advertisements 39, 40, 41, 42, 43, and 44 that were found in response to the query initiated by button 40. A scroll bar 45 shows that there are additional digital advertisements that are not shown. When link 46 is activated, the missing account information document shown in Figure 10 is returned by the merchant computer.

Figure 10 shows that the merchant computer has partial information on the buyer's account. Message 47 shows that the merchant computer already knows the buyer's account number. Purchase button 48 will send the optional user reference string in dialog box 50 to the merchant computer described by the URL behind button 48 and purchase the product corresponding to digital advertisement 39. Cancel link 49 will return the user to the document shown in Figure 2.

When purchase button 48 is activated, a document 51 is sent by the merchant computer and displayed by the buyer computer as shown in Figure 11.

Figure 12 shows an alternative method of processing a sales transaction. In this method when the user requests a purchase at 52, the buyer computer constructs a payment order at 53 and sends it for approval to the payment computer at 54. The payment computer authorizes the payment order at 55; and when the payment order is authorized, returns an unforgeable certificate at 56 that the payment order is valid. Means of creating such unforgeable certificates are described in authenticator method number one below. If at step 55 the payment order is not authorized, a rejection message is sent at 56 and the sales transaction is terminated.

The buyer computer then proceeds at 57 to send a pre-authorized purchase request to the merchant computer. The unforgeable certificate 56 is included in a purchase message at 57 that is sent at 58 to the merchant computer.

- 5 Based upon the pre-authorized payment order the merchant computer performs fulfillment at 59 and returns the product at 60. In a variation, the merchant computer at 59 checks to ensure the payment order has not been previously used. This can be accomplished by checking with a payment computer or maintaining a merchant computer database of previously accepted payment orders. The unforgeable certificate created at step 56 does not need to include the user account information. This variation is useful if the user wishes to make purchases and remain anonymous to the merchant.

15 A Network Payment System

- A network payment system 300 as shown in Figure 13, employs a public packet-switched network 69 to interconnect a plurality of client computers 70 and 71, and a plurality of payment computers such as 72, each payment computer having an account database 73, a settlement database 74, an authorized address database 75, a sender credential database 76, a financial system interface 77, and a real-time authorization interface 78. The interfaces 77 and 78 may be implemented by a single communications line.

In an alternate embodiment, the network payment system further includes external devices that are kept in the possession of users so that the users can authenticate themselves when they use a buyer computer.

5 Account database 73 maintains temporal spending amounts, such as the amount spent in the current day, and also maintains temporal spending limits. The account database may also maintain a translation between principal identifiers and external account identifiers. Settlement
10 database 74 records committed payment orders along with any authorization information for the orders that was obtained from interface 78. Address database 75 maintains for each sender a list of authorized buyer computer and delivery addresses. Credential database 76 maintains a list of
15 credentials for principals and information that can be used to authenticate principals.

Figure 14 is a flowchart that describes the operation of the payment system. A client computer 71 constructs a payment order at 79, and computes and adds an
20 authenticator to the payment order at 80. The payment order is sent at 81 to a payment computer, where the authenticator is verified at 82 to ensure that the payment order was originated by the sender it describes. Below we present different means of implementing 80 and 82.

101011121314151617181920

If the payment order is authentic and address restrictions are desired, at 83, either or both of the client computer address or the specified delivery address can be checked against address database 75. If address restrictions are desired and if the addresses in the payment order are not in the database, the payment computer sends a rejection message to the client computer. Address database 75 specifies, for each principal, acceptable client computer addresses and delivery addresses. A delivery address can be a network address, or a street address for packaged goods. As is known in the art, database 75 can include wild-card specifications and similar techniques to reduce its size. For example, database 75 could contain an entry for principal identifier "*@acme.com" restricting legal delivery addresses to "computer: *.com", "computer: cmu.edu", and "surface: *, 34 Main Street, Anytown, USA", indicating that any user at the company Acme can order products to be delivered to the network address at Acme or the university CMU, or to anyone at 34 Main Street, Anytown, USA.

If payment order address restrictions are not desired or have been checked, processing continues at 84 where the payment order is checked for replay and temporal spending limits. Replay is checked for by making sure that the sender did not previously present a payment order with

the same nonce by checking an index of committed payment orders by nonce in settlement database 74. If nonces are based on time, then a payment order that is older than an administratively determined value can be rejected out of
5 hand. Time based nonces or sequential nonces permit old nonces to be removed from the settlement database 74. If a payment order has been previously processed or its nonce is too old, the payment order computer sends a rejection message to the client.

10 After the payment order passes the replay check, temporal spending limits are checked in account database 73. These spending limits can be applied on a per sender, per group of senders, and per payment system basis to limit fraud risk. The limits can be applied to any duration of
15 time, for example a maximum spending amount per hour or per day. If the payment order would violate a spending limit, the payment computer sends a rejection message to the client.

Once the payment order passes the temporal spending
20 check at 84, a message is constructed at 85 to check that the external account that backs the sender's payment system account has adequate funds or credit. If the sender identifier in the payment order is not already an account number in the external financial system, it is translated
25 into a corresponding account number in the external

financial system using account database 73. A real-time authorization request message is sent at 86 to the external financial system over interface 78. If the external financial system approves authorization request 86, an
5 authorization message is returned at 87. If request 86 is not approved, the payment computer sends a rejection message to the client at 87.

In a variation of the above described approach, processing continues at 95 after 84. At 95 real-time
10 authorization is only obtained when the total of a sender's payments since the last real-time authorization reaches a preset value, or the payment order is over a preset amount. These preset values can be optionally recorded on a per principal basis in database 73 or can be administratively
15 determined for all principals. In this manner, the number of messages to the external financial system can be reduced. In addition, the payment system can avoid making real-time authorization requests for small payments when the risk is acceptable to the payment system operator. If real-time
20 authorization is necessary, processing continues at 85 after 95. If real-time authorization is not necessary for a request, at 100 the payment order amount is added to the sender's total of payments since the last real-time authorization in database 73, and processing continues at
25 88.

1
In another variation after 100 a check is made at
101 in database 73 to see if a background authorization
process should be scheduled. A background authorization
process permits the payment computer to continue its normal
5 processing while it checks with the financial authorization
network on the sender's account. This mechanism can be used
to limit payment system risk. If the background
authorization fails, the account is suspended by so updating
database 73. If the sender's total of payments since last
10 authorization is over a preset value stored in 73 then a
background authorization process is scheduled at 102.
Otherwise processing continues at 88.

In another variation, at 95 and 101 authorizations
are obtained based on the amount spent since last
15 authorization and time since last authorization.

At 88 the payment order is committed to execution
and is recorded in settlement database 74. Recorded with
the payment order in database 74 are portions of
authentication message 87 that show that the payment
20 computer contacted the remote financial system. The amount
of the payment order is added to running temporal spending
records in database 73, and an authorization message is sent
to the client computer at 90. The authorization message
includes the payment order. In an alternate embodiment, at
25 90 the authorization message contains a truncated payment

order that includes at least the payment order's sender and the payment order's unique nonce.

In an alternate embodiment, the authorization message sent to the client at 90 includes at least one legal
5 delivery addresses for the sender as determined from database 75.

Authorization message 90 must be transmitted in such a way that the client computer can be sure that it came from the payment computer. At 89 a payment system specific
10 authenticator is added payment order. At 91 this authenticator is checked by the client computer. The steps at 89 are a dual of step 80, and the steps at 91 are a dual of step 82. The authentication means for steps 89 and 91 are described below.

15 Finally, settlement is performed at 92 in the external financial system 77 between external accounts that correspond to the sender and the beneficiary. If settlement is accomplished as part of real-time authorization at steps 86 and 87, as may occur in a real-time debit network, then
20 no other steps need to be taken. If settlement is not accomplished as part of the authorization process, then financial system messages are sent to interface 77 to effect settlement. Depending on the external accounts involved, these messages may include electronic funds transfer
25 messages or automated clearinghouse messages.

In an alternate embodiment, at 92 settlement messages are sent to reconcile net transfer balances between principles on a temporal basis, for example once a day. In this embodiment the number of settlement messages can be
5 less than the number of payment orders.

Authenticators may be created and checked using one of the following methods. The payment computer can use any of the first four methods, and the client computer can use any of the methods described.

10 In a first method for authenticators, at steps 80 or 89, a digest of the payment order is signed by the sending computer using a public-key cryptographic system such as RSA. This signature is used as the authenticator. As is well known in the art, the signing can be accomplished using
15 a private key created from a public-key pair, where the signing key is only known by the signer, and the other public key is known to the receiving computer. At the payment computer the public key corresponding to each sender is kept in credential database 76. The private key for the
20 payment service is also kept in database 76. At steps 82 or 91, the signature of the received message is checked using the public key known to the receiving computer.

In a second method for authenticators, at steps 80 or 89, a digest of the payment order is signed by the
25 sending computer with a private key cryptosystem such as

DES. This signature is used as the authenticator. At the payment computer, the private key corresponding to each sender is kept in credential database 76. At step 80, a digest of the payment order is signed by the client

5 computer, and at step 89 a digest of the payment order with an added approval code is signed by the payment computer using the same private key. At steps 82 or 91, the signature of the received message is checked using the shared private key.

10 In a third method for authenticators, at step 80 the authenticator is computed by a protected device external to the system such as a Smart-Card. A protected device is specifically designed to be extremely difficult both to replicate and to compromise. In this method, the payment
15 order is communicated at 80 to a Smart-Card. The Smart-Card computes and signs a digest of the payment order, and then communicates the signature back at 80 to be used as an authenticator. A Smart-Card produced authenticator uniquely associates a payment order with its creating Smart-Card.

20 This is accomplished by having the Smart-Card contain a secret key "K" that is used to create a digital signature of the payment order. "K" is never released outside of the Smart-card. The Smart-Card is designed to make it computationally infeasible to compute "K" even with
25 possession of the device. In this method, at step 82, a

signature checking key from database 76 is used to check the authenticator. In an alternate embodiment, a user must manually signal their acceptance of each payment order on an input device that is part of the external device before the authenticator is created by the external device.

In a fourth method for authenticators, at steps 80 or 89, a network address is used as an authenticator. At steps 82 or 91, a digest of the payment order is sent back to the specified network address along with a random password. The computer at the specified network address must then return the payment order digest along with the password. If the network guarantees to deliver messages to the proper network address, this method will guarantee that the user or computer at the specified network address approves of the payment order. Assuming that network delivery is trusted, this method can be used to authenticate a sender computer's network address in a payment order. Alternatively, electronic mail can be used to send such confirmation messages between a user and the payment system.

In a fifth method for authenticators, at step 80, the authenticator is produced by an external device that produces a sequence of non-predicable transaction identifiers that are device specific. The authenticator is entered by the user into the client computer by reading its

display. One such device is described in U.S. Patent 4,856,062. According to this method, at step 91, the authenticator can be checked using the sender specific fixed code of the device which is kept in database 76. This
5 sequence of steps is also shown in Figure 15 at steps 93 and 94.

In a sixth method for authenticators, at step 80, the authenticator is obtained by querying the user for a transaction identifier that is the next string from a
10 physical list of one-time authorization strings. Such as list could be produced on a card, and the user can cross off authorization strings as they are used. According to this method, at step 91, the authenticator is checked against the next expected string from the sender using database 76.
15 Database 76 can hold for each sender a list of random authorization strings, or can hold a sender specific secret key that was used to generate the list of authentication strings along with how many strings have been used so far. This sequence of steps is also shown in Figure 15 at 93 and
20 94.

In a seventh method for authenticators, at step 80 the authenticator is a previously obtained personal identification number (PIN) for the user. In this method in 91 the authenticator is checked against the expected PIN for
25 the sender using database 76.

As will be obvious to one skilled in the art, any of the methods for creating authenticators can be used together to increase system security. For example, authenticator method six can be used to create an authenticator based on a transaction identifier, and then a payment order including a transaction identifier can be given a further authenticator using authenticator method one. In this example the resulting authenticators would be checked with their respective methods.

10 A digest of a payment order can be created with an algorithm such as MD5 [R. Rivest, The MD5 Message-Digest Algorithm, MIT Laboratory for Computer Science, Network Working Group Request for Comments 1321]. Alternatively, a digest can be the entire payment order or other functions of the payment order's component parts.

In addition in both the sales and payment systems alternate authenticator techniques can be used such as those described by Voydock and Kent in "Security Mechanisms in High-level Network Protocols", Computing Surveys Vol. 15, No. 2, June 1983. As will be appreciated by those skilled in the art, two-way authenticated byte-stream or remote procedure call interface connections that protect against replay can replace our message based authenticators.

Additions, subtractions, deletions, and other modifications of the described embodiment will be apparent

to those practiced in the art and are within the scope of
the following claims.